UDC 621.391

PROTECTION AGAINST THE EFFECT OF DIFFERENT CLASSES OF ATTACKS ON UAV CONTROL CHANNELS

Mykola M. Kaidenko, Serhii O. Kravchuk

Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. Protecting the data link of an unmanned aerial vehicle (UAV) is a top priority for countering attacks on UAVs. In this case, it should be taken into account that even the use of the most protected from the effects of deliberate interference types of modulation with spectrum spread does not guarantee the protection of such a channel.

Objective. The vulnerability of UAVs using cyber-attacks on a wireless channel is quite large, its study remains relevant, and therefore further development of complex effective means of countering such cyber-attacks is necessary, which is the purpose of this work. Moreover, the countermeasures presented in the work are based on the use of architectural solutions for building a UAV communication channel, which is different from traditional ones.

Methods. Structural-functional methods for constructing a secure wireless system of UAV communication channels are being investigated.

Results. A block diagram of the organization of UAV electronic countermeasures has been developed, which shows the data transmission channel from the UAV ground control station, the organization of the jamming channel, and the structure of the signal at the receiver input with all distortions and interference.

Interferences that can act as a signal of intentional interference from an electronic warfare station are presented and analysed.

An architectural solution is proposed using two channels in different frequency bands for the UAV control channel. A schematic structure of the organization of such a communication channel is presented. An expression is given for the margin of safety of a communication channel against a specific intentional interference. It is shown that the proposed architectural solution will have a similar effect when exposed to structured interference on the communication channel. In the case of the impact of imitation interference, the situation will be ambiguous, so it is very important to correctly determine the channel that is affected by intentional interference.

It is shown that to determine the presence of intentional interference, it is necessary to have at least one more degree of freedom, which is necessary for classifying such interference and effectively counteracting it. Such a degree of freedom can be achieved by additional dimensions or architectural solutions for building a communication system.

Conclusions. The types of intentional interference that can affect the UAV communication channel, the features of their application, and characteristics to ensure effective electronic protection are presented. Scenarios for counteracting the influence of attacks on UAV control channels are proposed. Scenarios with qualitative estimates are given, on the basis of which algorithms for detecting intentional interference and algorithms for counteracting the influence of such interference on the UAV communication channel can be built. It is assumed that the algorithms use averaged parameters, the length of the averaging interval is chosen as a multiple of the length of one data frame, which makes it possible to exclude from consideration fast fading in the communication channel that occurs in the case of frequency selective channels.

Keywords: *unmanned aerial vehicles; control channels; security; opposition; cyber attack.*

I. INTRODUCTION

In recent years, the use of unmanned aerial vehicles (UAVs) has become increasingly widespread for both military and civilian purposes. Such distribution will continue in the future due to the development and improvement of technologies for supporting the operation of UAV equipment, which leads to the creation of cheaper and more intelligent UAV systems [1-3]. However, the widespread UAV leads to an increase in the safety problems of their operation [4]. Thus, traditional autopilot designs are based on human control and often do not take into account cybersecurity threats, which makes them vulnerable to various kinds of attacks. For example, in 2009, a predator UAV was hijacked, which forced developers to pay attention to the cybersecurity of the UAV [5]. Cyber-attacks on UAVs can be divided into three main categories: hardware attacks, wireless attacks, and sensor spoofing (the practice of attackers masquerading as a specific user or device connected to a network). in hardware attacks, the attacker has access to the hardware components of the autopilot; while in wireless attacks, attackers use wireless communication channels to penetrate the system.

At present, UAV-related research on countering cybersecurity threats focuses mainly on GPS signal jamming and spoofing, but attacks on controls and data links are ignored. While the data link is the most vulnerable in terms of cyberattacks on UAVs, a gap in research on attacks on the data link is a concern, since the operator can see the UAV go astray due to a control channel attack, but is unable to detect this attack and resist it [6]. The results of tests conducted by independent security researchers have shown that drones are quite vulnerable [7]. In some cases, online resources even provide full source codes or tools that were used to carry out attacks on UAVs, containing ready-made background information about vulnerable drones and related attack tools. An example is the description of the US Air Force RQ-170 drone when the Iranian government claimed that it had captured the drone through its cyber warfare unit [8]. While there is some debate about the means of attack, the captured drone appears to be completely undamaged, meaning it was not hit by projectiles. With regard to civilian drones, the situation with attacks is much more complicated. So [9] announced Sky Jack, a dedicated drone hijacking platform exclusive to Parrot AR drones that exploit a Wi-Fi hotspot vulnerability in Parrot AR drones to take control of them.

Protecting the UAV data link is a top priority for countering attacks on UAVs. In this case, it should be taken into account that even the use of the most protected from the effects of deliberate interference types of modulation with spread spectrum does not guarantee the protection of such a channel. A lot of research shows that the transition to the frequency-hopping spread spectrum (FHSS) alone cannot completely protect the communication channel from hacking and suppression. So, in [10] several algorithms for cracking a pseudo-random sequence FHSS with external observation were presented, and in [11] the security of drone controllers that use frequency hopping spectrum (FHSS) was investigated. In the process of research using not the fastest software-defined radio (SDR) Universal Software Radio Peripheral (USRP), in comparison with [12], the hopping sequence of the target system was successfully extracted and the baseband signal was determined. In addition, high-energy broadband jammers can block the entire jump space used by the FHSS system. A random jammer with a much higher hopping speed can degrade the signal-to-noise ratio (SNR) [13].

The use of cryptographic algorithms to protect a wireless data transmission channel also cannot guarantee such a channel from “hacking”, especially for civilian UAVs, due to the fact that the key length is limited by law. In [14,15], studies are presented that have studied strategies for preventing attacks on wireless communications. Here are algorithms for detecting attacks that want to infiltrate and extract encryption keys. By extracting the encryption keys, attackers can inject their false data into the same correct data structure. In such attacks, the attackers introduce errors into the cryptographic algorithm to produce an erroneous ciphertext so that they can decode the encryption key.

Thus, it is obvious that the vulnerability of UAVs using cyber-attacks on a wireless channel is quite large, its study remains relevant, and therefore further development of complex effective means of countering such cyber-attacks is necessary, which is the purpose of this work. Moreover, the countermeasures presented in the work are based on the use of architectural solutions for building a UAV communication channel, which is different from traditional ones and was previously proposed in [16-18].

II. Interference affecting the UAV communication channel

In the general case, the effect of intentional interference on the UAV communication channel, regardless of the purpose of the UAV itself (military or civilian), is, in its own way, a means of electronic warfare. With regard to UAV communication channels, three components of such electronic warfare can be distinguished:

- passive radio-electronic support ESM (Electronic Support Measures);
- active radio-electronic suppression ECM (Electronic Counter Measures);
- countering radio-electronic countermeasures - radio-electronic protection ECCM (Electronic Counter-Counter Measures).

Passive radio-electronic support in relation to UAVs consists mainly in radio intelligence (Communications Intelligence - CI), which ensures the interception of signals, determining the direction of their arrival and their analysis. To solve these problems, both modern systems capable of detecting unusual and complex signals, and traditional means, including radio direction finders with remote control, are used. Radio intelligence tools build a representation of the signal in the frequency domain and/or in the time domain and decide on the type of transmission, frequency, modulation, and other parameters of the signal. This information is used to identify the emitter.

The peculiarity of the last two components is that the development of the equipment used for their

maintenance is accompanied by a constant competition one with the other. This feature, in general, corresponds to the global trend in the development of weapons and counter-weapons - from ancient times (a shield against a sword) to the present (an aircraft against an anti-aircraft gun, etc.). While in the field of electronic jamming systems are being developed that generate various kinds of interference and false radiation, in the field of electronic protection, tools are being developed to reduce the negative impact of these systems.

A typical scenario of electronic warfare is a confrontation between the forces and means of all three components: electronic support, electronic suppression, and electronic protection. Moreover, such a confrontation is accompanied by the constant development of the technical means of each of the components and the tactics of their use. The complexity of modern Electronic Warfare (EW) systems and the limited time to make a decision require maximum automation of means to counteract the effects of deliberate jamming. At the same time, an important aspect is that the software of the electronic protection system would be modifiable, that is, it would have an open architecture, presented, for example, in [12].

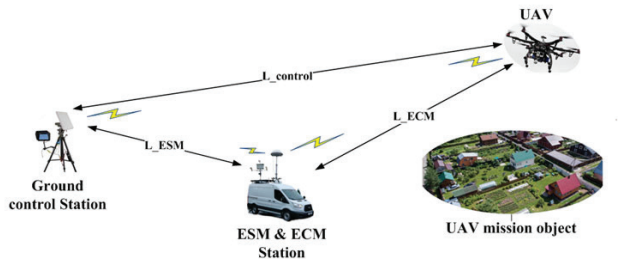

Fig. 1. Schematic representation of the organization of UAV electronic countermeasures

To ensure effective electronic protection, it is important to know what types of deliberate interference can affect the UAV communication channel, the features of their application, and its characteristics. Fig. 1 schematically shows the organization of UAV electronic countermeasures. To counter UAVs, electronic warfare stations are used that combine the functions of radio intelligence (Communications Intelligence) and radio suppression (Electronic Counter Measures), operating in a wide frequency range and allowing not only to jam UAV communication channels, for example [19] , but also small-sized low-power anti-drone gun with a limited frequency range, for example [20]. The electronic warfare station is always located closer to, or in close proximity to, UAV mission targets. As a result, the spatial and energy characteristics of the UAV communication channel and the suppression channel differ significantly in the length and direction of radiation.

Fig. 2 shows a block diagram of the organization of electronic countermeasures for an unmanned aerial vehicle, which shows the data transmission channel from the UAV ground control station, the organization of the jamming channel, and the structure of the signal at the receiver input with all distortions and interference.

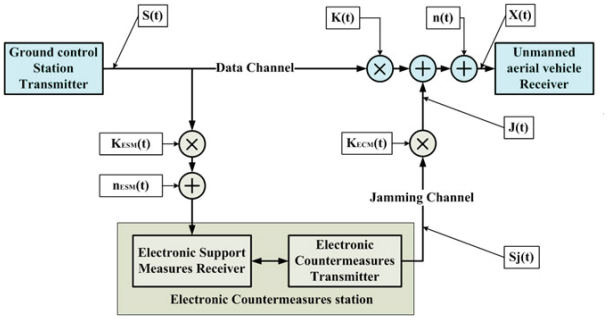

Fig. 2. Structural diagram of the UAV electronic countermeasures organization

The model of the transmitted signal from the ground control station to the UAV in the absence of radio interference in the general case can be described as:

$$X(t) = K(t) * S(t) + n(t), \quad (1)$$

where $X(t)$ - signal at the input of the receiver; $S(t)$ - useful signal; $K(t)$ is the coefficient that takes into account the influence of multipath in the channel; $n(t)$ is additive interference in a limited frequency band.

In the presence of radio interference, the channel model will be described as:

$$X(t) = K(t) * S(t) + n(t) + J(t), \quad (2)$$

where $J(t)$ is an additive signal from a radio countermeasures station, described in a general way.

In this case, the radio countermeasure channel, similarly to the communication channel with the UAV, can be affected by multipath and the receiver input receives additive interference, described as:

$$J(t) = K_{ECM}(t) * Sj(t) + n(t) \quad (3)$$

where $Sj(t)$ is the interference signal generated and emitted by the radio suppression station; $K_{ECM}(t)$ is a coefficient that takes into account the influence of multipath in the radio countermeasure channel.

It should be noted that the additive interference $n(t)$ in expressions (2) and (3) is the same interference, limited in frequency band by the input path and the main selection filters of the UAV receiver.

A signal is received at the receiver input of the radio intelligence station, which can be described similarly to (1). Ideally, the radio intelligence station recognizes the presence of the UAV control signal, classifies it, and determines its parameters (carrier frequency, modulation type, transmission rate). Since the requirements for the reaction time of the radio reconnaissance station and the inclusion of the radio suppression system are not “hard” compared to those for electronic warfare radar systems, real-time signal processing is not required and can be performed with a recorded signal fragment. After that, the electronic warfare station generates a jamming signal. The following interference can be used as such a signal.

Energy noise interference (broadband or narrowband). In the first approximation, it can be considered as a uniform "white noise" emitted in the operating frequency range of the UAV control station (broadband interference) or in the operating frequency band of the control channel (narrowband interference). The use of broadband interference requires high power from the station to achieve N_0 sufficient to provide SNR < SNR_{min}, at which the probability of erroneous reception by the UAV receiver BER is guaranteed to exceed the specified level (less than 10^{-3}).

Energy structured interference that is emitted at the operating frequency of the UAV control channel and repeats its parameters (type of modulation, frequency band). The impact of such interference on the communication channel leads to a breakdown of synchronization (frequency, phase, time) and the complete destruction of the information message. The results of testing the impact of such interference on a communication channel with QPSK modulation showed that a partial loss of synchronization in the communication channel occurs already at signal-to-interference ratio P_s/P_j = 10 dB, and a complete destruction of the channel at P_s/P_j = 6 dB. These tests were carried out using the Arradio SDR transceivers [21] as the main and Pluto SDR [22, 23] as the interference source, while the distance from the transmitters to the receiver was the same. For comparison, as a result of similar tests of the impact on the channel, limited in band by the filters of the additive white noise receiver, a partial loss of synchronization occurred at P_s/P_j = -3 dB, a complete destruction of the channel at P_s/P_j = -6 dB.

Imitation interference of the replay attack type, in which a recording of a real signal in a communication channel (for example, with a straight-line UAV movement) is used as an interference signal, which repeats the entire structure of the signal, including the elements of the channel cryptoprotection. For the effective impact of such interference on the communication channel, the condition $P_j/P_s > P_{j\min}$ ($P_{j\min}$ is the minimum interference power) must be satisfied at the receiver input. The test results in a communication channel with QPSK modulation without error-correcting coding showed that $P_{j\min}$ was 10 dB with an error probability BER < 10^{-3}.

Imitation interference of full or partial replacement of an informational message through the introduction of erroneous data (false data injection attack). This type of interference is the most harmful from the point of view of the "survivability" of the UAV, since it allows you to completely take control of the unmanned vehicle. To implement this type of interference, the radio intelligence station must fully detect the information message, including cryptoprotection, and then generate a new message with a modified one. For the effective impact of such interference on the communication channel, the condition $P_j/P_s > P_{j\min}$ must also be satisfied.

III. SCENARIOS TO COUNTER THE EFFECT OF ATTACKS ON UAV CONTROL CHANNELS

In [16-18], an architectural solution was proposed using two channels in different frequency bands for the UAV control channel. In this case, information in both channels is transmitted simultaneously with full duplication, which should increase the resistance of such a communication channel to the effects of deliberate interference. Schematically, the structure of the organization of such a communication channel is shown in Fig. 3.

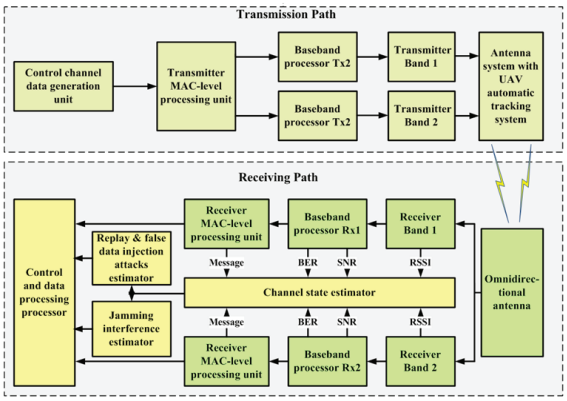

Fig. 3. Structural diagram of the organization of the UAV communication channel with protection against the effects of intentional interference

In [24], the anti-jam margin is described, which describes the stability of the system against attempts to suppress the signal. Although the use of this term is not always correct, it can be applied in general to denote a margin of safety against a specific jamming.

For a traditional version of the communication system, the anti-jam margin, which is affected by deliberate interference, can be described as:

$$M_{AJ} = \left(\frac{E_b}{(N_0 + J)}\right)_{\text{Received}} - \left(\frac{E_b}{(N_0 + J)}\right)_{\text{Required}} \quad (4)$$

For the variant proposed in [16-18] with two receiving channels in which the same information is transmitted, the anti-jam margin can be represented as:

$$M_{AJ} = \max(M_{AJ\_Channel1}, M_{AJ\_Channel2}) \quad (5)$$

Therefore, if intentional interference affects only one of the channels, the anti-jam margin will be maximum and limited only by unintentional interference in the range of the channel, in which there is no intentional interference. In the event of intentional interference on both receiving channels, in order to ensure high reliability of information transmission in the control channel and, accordingly, the "survivability" of the UAV communication channel and the UAV itself, it is sufficient to provide sufficient anti- jam margin, at least in one of the receiving channels.

Despite the fact that expressions (4) and (5) quite informatively describe the anti-jam margin in case of impact on the communication channel of energy interference, the proposed architectural solution will have a similar effect when the communication channel is exposed to structured interference. In this case, the next very important task of the receiver is to recognize the presence of intentional interference in the communication channel. In the case of the impact of energy interference (both noise and structured), this task is not particularly relevant, since deliberate interference only leads to loss of control of the UAV, is easily detected, and the means of counteracting the impact of such interference can be the transfer of the UAV to an autonomous flight mode. In the case of the impact of imitation interference such as replay attacks, or false data injection attacks, the situation becomes ambiguous, so it is very important to correctly determine the channel that is affected by deliberate interference and thus the attack on the UAV is carried out.

To effectively counter the effects of intentional interference, it is necessary to detect this interference and, if possible, classify it in order to correctly select and activate the necessary counteraction algorithm. A modern receiver includes several means of estimating the state of a communication channel: Received Signal Strength Indication (RSSI), signal-to-noise ratio (SNR), and error rate (BER).

The received signal strength indicator RSSI measures the amount of received signal in a particular frequency band as the total power of the received signal receivers. In this case, it is not determined whether the signal is useful, is an interference signal, or is a mixture of a signal with interference.

The ratio of the received signal power to the noise power SNR determines the quality of the received useful signal, provided that this signal is useful (detected) and a mixture of signal and interference is received, without specifying the type of interference. The term CINR (Carrier to Interference + Noise Ratio) is often used in the literature, which is synonymous with SINR (Signal Interference + Noise Ratio). The difference between SNR and SINR is only that SNR determines the ratio of signal power to the noise power, and SINR is the ratio of signal power to noise power and that interference resulting from interference, which is perceived in the same way as noise.

In the case of the presence of intentional interference in the mixture of signal and noise, there is no response at the RSSI measurement level to the presence or absence of such interference. At the level of SNR measurement, it is only possible to give an unambiguous answer to the signal quality and, as a result, to the presence of interference without classifying the type of interference.

Measurement of BER (counting the number of errors per frame interval N_{error}) is possible in communication channels with FEC (Forward Error Correction) error-correcting coding and allows you to more accurately determine the quality of the received signal compared to SNR, since it determines the quality of the received information. In addition, SNR measurements at low signal-to-noise ratios can have a significant error, regardless of whether the transmitted information is known (Data-Aided) [25] or unknown (Non-Data-Aided) [26-28]. Thus, BER can be a means of indicating the presence of SNR measurement error.

The above indicates that in order to determine the presence of intentional interference, it is necessary to have at least one more degree of freedom necessary for classifying such interference and effectively counteracting it. Such a degree of freedom can be achieved by additional measurements, and/or architectural solutions for building a communication system. The presence of the third degree of freedom

when using the architectural solutions proposed in [16-18] makes it possible to build algorithms for detecting intentional interference and counteracting their impact on the communication channel.

In the case of detecting a potential impact of intentional interference on the control channel, there are two options for more accurate detection of the impact of such interference: with feedback (Close Loop detection) and without feedback (Open Loop detection). At first glance, the feedback option is preferable, but it has its drawbacks since the impact can be carried out not only on the control channel but also on the telemetry channel. This detection option is applicable to small commercial UAVs that use the simplest communication system using only one frequency band for the control channel and telemetry. For small-sized civil and military UAVs that use two communication channels in different frequency bands to build the UAV control channel, it is preferable to use detection without feedback (Open Loop detection). For UAVs in which two communication channels in different frequency bands are fully used to build the UAV control channel and the telemetry channel, it is possible to use either one or the other option, their combination or simultaneous use. Open-loop detection has a significant advantage in the case of using two communication channels since it allows you to determine the channel with reliable information with minimal delay. However, the use of a combined scheme, when open-loop detection is used to make a decision about the impact of interference with confirmation of the decision made by the feedback channel, provides the highest probability of detecting the potential impact of intentional interference.

Table 1 shows scenarios with qualitative estimates, on the basis of which algorithms for detecting intentional interference and algorithms for counteracting the influence of such interference on the UAV communication channel can be built. It is assumed that the algorithms use averaged parameters, the length of the averaging interval is chosen as a multiple of the length of one data frame, which makes it possible to exclude from consideration fast fading in the communication channel that occurs in the case of frequency selective channels. In addition, the power of both communication channels must be chosen in such a way as to ensure the same energy potential in both channels, which will be used as one of the criteria for detecting deliberate interference.

Scenarios are written under the condition that the potential impact of intentional interference on the control channel is detected. The most accurate initial sign of detection is to control the difference between information messages in two communication channels:

$$Jam\_d = XOR\left(Message_{Channel1}, Message_{Channel2}\right). \quad (6)$$

If $J_{am\_d} = 1$, then it is likely that one of the communication channels may be subject to a deliberate attack.

Table 1.

Scenario	Interference type	Description of symptoms
1	Energy noise interference broadband	In one of the channels $N_{error} >> 1$; $RSSI_{Chan\_error} > RSSI_{Chan\_correct}$; $SNR_{Chan\_error} < SNR_{Chan\_correct}$; $RSSI_{Chan\_error+-BW} \sim RSSI_{Chan\_error}$
2	Energy noise interference narrowband	In one of the channels $N_{error} >> 1$; $RSSI_{Chan\_error} > RSSI_{Chan\_correct}$; $SNR_{Chan\_error} < SNR_{Chan\_correct}$; $RSSI_{Chan\_error+-BW} << RSSI_{Chan\_error}$
3	Energy structured interference	In one of the channels $N_{error} >> 1$; $RSSI_{Chan\_error} >= RSSI_{Chan\_correct}$; $SNR_{Chan\_error} <= SNR_{Chan\_correct}$; No Frame Synchronization (Packets)
4	Imitation interference such as replay attack	$N_{error\_Chan1} \sim N_{error\_Chan2}$; $RSSI_{Chan1} >> RSSI_{Chan2}$; $SNR_{Chan1} >= SNR_{Chan2}$; Incorrect order of imitation inserts
5	Imitation noise replacement (false data injection attack)	$N_{error\_Chan1} \sim N_{error\_Chan2}$; $RSSI_{Chan1} >> RSSI_{Chan2}$; $SNR_{Chan1} >= SNR_{Chan2}$; Observation of changes over a long time interval

As can be seen from the table for energy noise interference scenarios, the first sign is the presence in one of the channels of a large number of bit errors that cannot be corrected by error-correcting coding. The next sign is the excess of the level of the received RSSI signal in this channel over the RSSI in the channel with normal signal reception. The SNR of an errored channel (if it can be measured) will be substantially less than the SNR of an error-free channel. Checking for the presence of broadband or narrowband energy interference, if necessary, can be carried out by tuning to an adjacent frequency channel within the operating frequency range, while for broadband interference RSSI will be practically unchanged. In the presence of fading in the channel, which is not affected by interference, the behaviour of signs of the presence of interference will be similar to the case without fading. Deep fading can lead to temporary destruction of the channel, however, observation over a long-time interval allows you to accurately determine the channel affected by energy noise interference.

For the energy structured interference scenario, there will also be a large number of bit errors in the affected channel. In this case, the RSSI of the channel affected by the interference can be commensurate with the RSSI in the channel with normal signal reception. SNR can also be comparable in both channels and is highly dependent on how it is measured. Thus, the second sign is the structure of the data frame, or rather the impossibility of frame synchronization.

A scenario using simulated interference such as a repetition attack will be characterized by the absence of errors in both channels, the SNR will be commensurate or at a level sufficient for stable reception, while the RSSI in the channel with interference will exceed that of the channel without interference by a level sufficient to suppress the correct signal. The main sign of the presence of a repetition attack will be the correctness of the sequence of imitation inserts, the repetition period of which should be sufficiently large. Similar signs will also characterize the channel with imitation interference of substitution, however, in this case, imitation inserts can also be replaced, therefore, to determine the sign of the presence of interference, it is necessary to observe changes in the behaviour of the communication channel over a long-time interval.

IV. CONCLUSION

The types of intentional interference that can affect the UAV communication channel, the features of their application, and characteristics to ensure effective electronic protection are presented.

A block diagram of the organization of UAV electronic countermeasures has been developed, which shows the data transmission channel from the UAV ground control station, the organization of the jamming channel, and the structure of the signal at the receiver input with all distortions and interference.

Interferences that can act as a signal of intentional interference from an electronic warfare station are presented and analysed: energy noise interference (broadband or narrowband); energy structured interference, which is emitted at the operating frequency of the UAV control channel and repeats its parameters; imitation interference such as replay attack; imitation interference of complete or partial replacement of an information message by introducing erroneous data (false data injection attack).

Scenarios for counteracting the influence of attacks on UAV control channels are proposed.

An architectural solution is proposed using two channels in different frequency bands for the UAV control channel. A schematic structure of the organization of such a communication channel is presented. An expression is given for the margin of safety of a communication channel against a specific intentional interference. It is shown that the proposed architectural solution will have a similar effect when exposed to structured interference on the communication channel. In the case of the impact of imitation interference, the situation becomes ambiguous, so it is very important to correctly determine the channel that is affected by deliberate interference and thus the attack on the UAV is carried out.

It is shown that in order to determine the presence of intentional interference, it is necessary to have at least one more degree of freedom, which is necessary for classifying such interference and effectively counteracting it. Such a degree of freedom can be achieved by additional dimensions or architectural solutions for building a communication system.

Scenarios with qualitative estimates are given, on the basis of which algorithms for detecting intentional interference and algorithms for counteracting the influence of such interference on the UAV communication channel can be built. It is assumed that the algorithms use averaged parameters, the length of the averaging interval is chosen as a multiple of the length of one data frame, which makes it possible to exclude from consideration fast fading in the communication channel that occurs in the case of frequency selective channels.

REFERENCES

1. S.O. Kravchuk, I.M. Kravchuk, “Using RFID technology at operating a drone swarms in communication system mode”, Information and telecommunication sciences: international research journal, Vol. 11, N. 2 (21), pp. 16-23, (2020), https://doi.org/10.20535/2411-2976.22020.16-23.

2. S. Kravchuk, L. Afanasieva, “Formation of a wireless communication system based on a swarm of unmanned aerial vehicles”, Information and Telecommunication Sciences, No 1, pp. 11-18 (2019), https://doi.org/10.20535/2411-2976.12019.11-18

3. M. Ilchenko, S. Kravchuk, Mobile infocommunication systems, Information and Telecommunication Sciences, Vol. 11, No 1, pp. 11-19 (2020), https://doi.org/10.20535/2411-2976.12020.11-19

4. J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations”, Internet of Things, **11** (2020), https://doi.org/10.1016/j.iot.2020.100218

5. A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge, “Cyber-attack vulnerabilities analysis for unmanned aerial vehicles”, Infotech Aerospace, 9 June 2012 - 21 June 2012, Garden Grove, California (2012), https://doi.org/10.2514/6.2012-2438.

6. C.G. L. Krishna, R.R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles", 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), 2017, pp. 194-199, https://doi.org/10.1109/SSRR.2017.8088163.

7. S. Walters, “The updated list of vulnerable drones & attack tools”, [online] (2021), https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809.

8. Iran-U.S. RQ-170 incident, Wikipedia - the free encyclopedia [online] (2015), https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

9. S. Kamkar, “SkyJack”, [online] (2015) http://www.samy.pl/skyjack/

10. M. Song, T. Allison, “Frequency hopping pattern recognition algorithms for wireless sensor networks”, In: ISCA., pp. 264–269 (2005), https://www.semanticscholar.org/paper/Frequency-Hopping-Pattern-Recognition-Algorithms-Song-Allison/44726f65e6f65ad16c98ee8ca694094636e83712

11. H. Shin, K. Choi, Y. Park, J. Choi, Y. Kim, “Security Analysis of FHSS-type Drone Controller”, in: Kim H., Choi D. (eds) Information Security Applications. WISA 2015. Lecture Notes in Computer Science, vol 9503. Springer, Cham. (2016), https://doi.org/10.1007/978-3-319-31875-2_20

12. M.M. Kaidenko, D.V. Roskoshnyi, “Software Defined Radio in Communications”, in: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham (2019), https://doi.org/10.1007/978-3-030-16770-7_11, Print ISBN 978-3-030-16769-1

13. M. Stahlberg, “Radio jamming attacks against two popular mobile networks”, Tik-110.501 “Seminar on Network Security”, Vol. 3 (2000), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.7211&rep=rep1&type=pdf

14. J. Dofe, J. Frey, H. Pahlevanzadeh, Q. Yu, “Strengthening SIMON Implementation Against Intelligent Fault Attacks”, IEEE Embedded Systems Letters, 7(4), p. 113-116, (2015), https://doi.org/10.1109/LES.2015.2477273

15. B. Wang, L. Liu, C. Deng, M. Zhu, S. Yin, S. Wei, “Against Double Fault Attacks: Injection Effort Model, Space and Time Randomization Based Countermeasures for Reconfigurable Array Architecture”, IEEE Transactions on Information Forensics and Security 11(6):1-1(2016), http://dx.doi.org/10.1109/TIFS.2016.2518130

16. M. Kaidenko, S. Kravchuk, “Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio”, In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. (2021), https://doi.org/10.1007/978-3-030-58359-0_16

17. M.M. Kaidenko, S.O. Kravchuk, "Anti-Jamming System for Small Unmanned Aerial Vehicles", 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD), 19-21 Oct. 2021, Kyiv, Ukraine (2021), https://doi.org/10.1109/APUAVD53804.2021.9615403.

18. M. Kaidenko, S. Kravchuk, "Creation of communication system for unmanned aerial vehicles using SDR and SOC technologies," 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2019, pp. 1-4, https://doi.org/10.1109/UkrMiCo47782.2019.9165422.

19. "Groza-S" counter-UAV electronic warfare station (mounted onto military vehicles), https://www.armour.gr/catalogues/pdf/Groza-S.pdf

20. REX-2 [online], https://zala-aero.com/production/means-of-ew/rex-2/

21. HSMC ARRadio Daughter Card [online], https://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&No=946

22. ADALM-PLUTO. Software-Defined Radio Active Learning Module [online], https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview

23. S.O. Kravchuk, M.M. Kaidenko, I.M. Kravchuk, “Experimental Development of Communication Services Scenario for Centralized and Distributed Construction of a Collective Control Network for Drone Swarm”, 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD), 19-21 Oct. 2021, Kyiv, Ukraine (2021), https://doi.org/10.1109/APUAVD53804.2021.9615433

24. B. Sklar, Digital Communications: Fundamentals and Applications, Second Edition, Prentice-Hall, Upper Saddle River, NJ, 2001.

25. A. Wiesel, J. Goldberg, H. Messer-Yaron, "SNR estimation in time-varying fading channels", in IEEE Transactions on Communications, vol. 54, no. 5, pp. 841-848, May 2006, http://dx.doi.org/10.1109/TCOMM.2006.873995.

26. Z. Sun, X. Gong, F. Lu, “A non-data-aided SNR estimator based on maximum likelihood method for communication between orbiters”, J Wireless Com Network, 123 (2020). https://doi.org/10.1186/s13638-020-01730-4

27. D. R. Pauluzzi, N. C. Beaulieu, “A comparison of SNR estimation techniques for the AWGN channel”, IEEE Transactions on Communications, Vol. 48, No. 10, p.1681-1691 (2000).

28. F. Harris, C. Dick, “SNR estimation techniques for low SNR signals”, 15 th International Symposium on Wireless Personal Multimedia Communications (WPMC), Taipei, Taiwan, 24-27 Sept. 2012, p.276-280 (2012), https://ieeexplore.ieee.org/abstract/document/6398797

Кайденко М.М., Кравчук С.О.

Захист від впливу різного класу атак на канали управління БПЛА

Проблематика. Захист каналу передачі безпілотного літального апарату (БПЛА) є першочерговим завданням для забезпечення протидії атакам на БПЛА. При цьому треба враховувати, що навіть використання найбільш захищених від впливу умисних завад видів модуляції з розширенням спектра не гарантує захисту такого каналу.

Мета дослідження. Вразливість БПЛА з використанням кібератак на бездротовий канал досить велика, її дослідження залишається актуальним і тому потрібна подальша розробка комплексних ефективних засобів протидії таким кібератакам, що є метою справжньої роботи. Причому представлені в роботі засоби протидії базуються на використанні архітектурних рішень щодо побудови каналу зв'язку БПЛА, які відмінні від традиційних.

Методика реалізації. Досліджуються структурно-функціональні методи побудови безпроводової захищеної системи каналів зв'язку БПЛА.

Результати дослідження. Розроблено структурну схему організації радіоелектронної протидії БПЛА, в якій представлено канал передачі даних від наземної станції управління БПЛА, організацію каналу постановки завади та структуру сигналу на вході приймача з усіма спотвореннями та завадами.

Представлені та проаналізовані завади, які можуть виступати як сигнал навмисної завади станції радіоелектронної боротьби.

Запропоновано архітектурне рішення із використанням двох каналів у різних діапазонах частот для каналу управління БПЛА. Подано схематичну структуру організації такого каналу зв'язку. Дано вираз запасу міцності каналу зв'язку проти конкретної навмисної завади. Показано, що запропоноване архітектурне рішення матиме аналогічний ефект при впливі на канал зв'язку структурованих завад. У разі впливу імітаційної завади ситуація буде неоднозначною, тому дуже важливо правильно визначити канал, на який впливає навмисна завада.

Показано, що для визначення присутності навмисної завади необхідно мати ще як мінімум один рівень свободи, необхідний для класифікації такої завади та ефективної протидії їй. Такий ступінь свободи може бути досягнутий додатковими вимірами, або архітектурними рішеннями щодо побудови системи зв'язку.

Висновки. Подано типи навмисних завад, які можуть діяти на канал зв'язку БПЛА, особливості їх застосування та характеристики для забезпечення ефективного радіоелектронного захисту. Запропоновано сценарії протидії впливу атак на канали управління БПЛА. Наведено сценарії з якісними оцінками, на основі яких можуть будуватись алгоритми детектування навмисних завад та алгоритми протидії впливу таких завад на канал зв'язку БПЛА. Передбачається, що для роботи алгоритмів використовуються усереднені параметри, довжина інтервалу усереднення вибирається кратною довжиною одного кадру даних, що дозволяє виключити з розгляду швидкі завмирання в каналі зв'язку, що виникають у разі частото-селективних каналів.

Ключові слова: *безпілотні літаючі апарати; канали передачі даних; безпека; протидія; кібератака.*